REMARKS

The Office Action mailed February 18, 2010, has been carefully considered. Reconsideration in view of the following remarks is respectfully requested.

Record of Interview

On February 25, 2010, an interview was conducted by telephone between Examiner Chan and the undersigned. The Applicant thanks the Examiner for granting this interview. The details of the interview are set forth in the Interview Summary document made of record.

Claim Status and Amendment of the Claims

Claims 1-2, 5-12, 15-21, 24-29, 31-39, and 41 are currently pending.

No claims stand allowed.

Claims 3-4, 13-14, 22-23, 30 and 40 were previously cancelled without prejudice or disclaimer of the subject matter contained therein.

Claims 1, 11, 20, and 31 are hereby amended to clarify the recitations per the Examiner's suggestions, and not for overcoming prior art or other patentability reasons. Support for these changes is found in the specification, figures, and claims as originally filed. The Amendment also contains minor changes of a clerical nature. No "new matter" has been added by the Amendment.

The First 35 U.S.C. § 103 Rejection

Claims 1-2, 5-12, 15-21, 24-29, and 31-41 stand rejected under 35 U.S.C. § 103 as allegedly being unpatentable over Meier et al.,[1] in view of Palekar et al.,[2] and further in view of

[1] U.S. Publication No. 2005/0185626 to Meier et al.

Kalavade et al.,[3] among which claims 1, 11, 20, 31, 32, 36, and 41 are independent claims.[4] This rejection is respectfully traversed.

As an initial matter, the Applicant notes Claim 40 was previously cancelled without prejudice or disclaimer of the subject matter contained therein. The Applicant assumes the Examiner intended to reject Claims 1-2, 5-12, 15-21, 24-29, 31-39, and 41.

Turning to the substance of the rejection, according to the M.P.E.P.,

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure.[5]

Furthermore, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination.[6]

Claim 1

Claim 1 as presently amended recites:

> A computer implemented method comprising:
> at a network access device communicably coupled to a host network, sensing a user device coupled to a port of the network access device;
> determining, by the network access device, if the user device supports a user authentication protocol used by the host network, the determining comprising polling the user device for the user authentication protocol, the user

[2] U.S. Publication No. 2003/0226017 to Palekar et al.
[3] U.S. Patent Publication No. 20030051041 to Kalavade et al.
[4] Office Action mailed February 18, 2010, at p. 3.
[5] M.P.E.P. §2143.
[6] *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

authentication protocol comprising a protocol to validate the identity of a user of the user device; and

placing, by the network access device, the port into a semi-authorized access state if the determining indicates that the user device does not support the user authentication protocol, the semi-authorized access state providing the user device with limited network access.

The Examiner states:

Meier et al. clearly disclose and show a computer implemented method comprising:

at a network access device (fig. 3 (1 02)) communicably coupled to a host network (paragraph 0004 (network)), sensing a user device (fig. 3 (302), paragraph 0032 (WSTA attempting to gain access to AP)) coupled to a port of a network access device (paragraph 0032 (attempting to gain access to AP)); and

placing the port into a semi-authorized access state (paragraph 0022 (default guest set)) the semi-authorized access state providing the user device with limits access (paragraph 0022 (restricted access)).

However, Meier et al. do not specifically disclose determining if said user device supports a user authentication protocol.

In the same field of endeavor, Palekar et al. clearly show determining if the user device supports a user authentication protocol used by the host network (para. 0049 (if user supports authentication protocol)), the determining comprising polling the user device for the user authentication protocol (para. 0049 (send a EAP request)), the user authentication protocol comprising a protocol to validate the identity of a user of the user device (para. 0044(user's identity));

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, and show determining if said user device supports a user authentication protocol, as taught by Palekar, so that proper access can be granted according to authentication.

However, Meier et al., as modified by Palekar, do not specifically disclose the determining the support of authentication is by the network access device and placing the port in a semi authorized state is by the network access device.

In the same field of endeavor, Kalavade et al. clearly show the determining the support of authentication is by the network access device (para. 0018 (authentication within a hotspot)) and placing the port in a semi authorized state is by the network access device (para. 0073 (without SIM support, use LAN-based authentication); para. 0058 (LAN protocol uses RADIUS); para. 01 69 (provide acces to limited services only)).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of invention to demonstrate a method of user authentication, as taught by Meier, show determining if said user device supports a user authentication protocol, as taught by Palekar, and show determining the support of authentication by the network access device and placing semi-authorized

> access on a port by the network access device, as taught by Kalavade, so that proper access can be granted according to authentication.[7]

Meier et al. in View of Palekar et al. and Further in View of Kalavade et al. Does Not Disclose Determining, By The Network Access Device, If The User Device Supports A User Authentication Protocol Used by the Host Network

Contrary to the Examiner's statement, Meier et al. in view of Palekar et al. and further in view of Kalavade et al. does not disclose "… determining if the user device supports a user authentication protocol used by the host network" as required by Claim 1. In support of the Examiner's statement, the Examiner refers to the following portion of Palekar et al.:

> [0049] After the TLS tunnel, or similar networking protocol, has been established, encrypting communication between the user's computing device and the authenticating server, intermediate devices, such as the access point, can no longer meaningfully observe the network communication between the two endpoints because they do not have the necessary cryptographic keys. At this point, a protocol such as EAP can be used to again negotiate an exact protocol for authenticating the user to allow the user access to the network. For example, using the encrypted communication between the user's computing device and the authenticating server, the authenticating server can send an EAP request for a particular authentication protocol, such as CHAP or MSCHAP. If the user's computing device supports the authentication protocol specified in the EAP request, it can respond with an acknowledgement. Once the exact authentication protocol is agreed upon, the user can be prompted for their identification. Because the authentication communications are now being sent as encrypted communications, the user can safely transmit their entire user id, such as their email address. Based on this information, the user's computing device can prove knowledge of the user's password by, for example, sending a key-hash of a server-sent random value, using the password, which the authentication server can verify and thereby authenticate the user and grant the user access to the network.[8]

The above portion of Palekar et al. cited by the Examiner speaks generally about using an encrypted communication between a user device and an *authenticating server* to negotiate a protocol for authenticating a user. The cited portion of Palekar et al. says nothing about determining, *by the network access device,* whether a user device supports a particular user

[7] Office Action at pp. 3-4.
[8] Palekar et al. at ¶ 49.

authentication protocol. The Applicant respectfully submits it is improper to equate a network access device with the authenticating server of Palekar et al.

Claim 1 was previously amended to make this distinction more clear. Specifically, Claim 1 was previously amended to recite in part "determining, *by the network access device,* if the user device supports a user authentication protocol used by the host network, the determining comprising polling the user device for the user authentication protocol, the user authentication protocol comprising a protocol to validate the identity of a user of the user device." (emphasis added)

Meier et al. in View of Palekar et al. and Further in View of Kalavade et al. Does Not Disclose Placing, by the Network Access Device, the Port Into a Semi-authorized Access State if the Determining Indicates That the User Device Does Not Support the User Authentication Protocol, the Semi-authorized Access State Providing the User Device with Limited Network Access

Contrary to the Examiner's statement, Meier et al. in view of Palekar et al. and further in view of Kalavade et al. does not disclose or suggest placing, by the network access device, the port into a semi-authorized access state if it is determined that the user device does not support the user authentication protocol, the semi-authorized access state providing the user device with limited network access, as required by Claim 1. In support of the Examiner's statement, the Examiner refers to the following portions of Kalavade et al.:

> [0018] In accordance with one or more embodiments of the invention, a method is provided for allowing multiple wireless operators to provide integrated authentication and billing services for respective subscribers within one wireless LAN hotspot. The method includes: (a) modifying a hotspot authentication server to support multiple operators by assigning a separate network access identifier for each operator; (b) associating a gateway of each operator with each respective network access identifier; and (c) forwarding authentication requests received by

> the authentication server to appropriate gateways, depending on the operator selected by the user, each selected gateway providing authentication and billing for the selected user.[9]
>
> [0058] Cellular users or WAN subscribers are typically authenticated in the WAN through the WAN operator's HLR, which contains user profile information as well as authentication parameters.[10]
>
> [0073] The authentication scheme in accordance with the various embodiments generally falls into three broad categories. The first category of authentication is designed for terminals without SIM support. The authentication mechanism can use the WAN database for service creation. Subsequently, the scheme uses a LAN-based login/password scheme for authentication. This scheme can also use LAN-based authentication protocols such as 802.1x.[11]
>
> [0169] Note that in this case, the user can also create a login/password in addition to the SIM authentication. This would be similar to the first case described earlier. This will allow the user to login even when his SIM may not be available. If desired, this can provide access to limited services only.[12]

The above portions of Kalavade et al. speak generally about modifying a hotspot authentication server to support multiple operators by assigning a separate network access identifier for each operator, associating a gateway of each operator with each respective network access identifier, and forwarding authentication requests received by the authentication server to appropriate gateways, depending on the operator selected by the user, but nowhere do the cited portions of Kalavade et al. disclose or suggest determining, *by the network access device*, if the user device supports a user authentication protocol used by the host network as required by Claim 1. (emphasis added) The Applicant respectfully submits it is improper to equate modifying a hotspot authentication server to support multiple operators, with determining, by the network device, if the user device supports a user authentication protocol used by the host network as required by Claim 1.

[9] Kalavade et al. at ¶ 18.
[10] Kalavade et al. at ¶ 58.
[11] Kalavade et al. at ¶ 73.
[12] Kalavade et al. at ¶ 169.

Nor do the cited passages disclose or suggest placing, *by the network access device*, the port into a *semi-authorized access state* if it is determined that the user device does not support the user authentication protocol, the semi-authorized access state providing the user device with limited network access, as required by Claim 1. (emphasis added) The cited passages speak generally about authentication, but say nothing about a *semi*-authorized access state.

Claim 1 was also previously amended to recite in part "placing, *by the network access device*, the port into a semi-authorized access state if it is determined that the user device does not support the user authentication protocol, the semi-authorized access state providing the user device with limited network access." (emphasis added) With this Amendment, Claim 1 has been further amended to clarify that the determination referred to in the "placing" step is the "determining" step. Specifically, Claim 1 has been amended to recite in part "placing, by the network access device, the port into a semi-authorized access state if *the determination indicates* that the user device does not support the user authentication protocol, the semi-authorized access state providing the user device with limited network access." (emphasis added) These amendments clearly indicate it is the network access device that performs the recited (1) sensing, (2) determining, and (3) placing steps in Claim 1. These three steps, each being performed by the network access device as required by Claim 1, is not taught or suggested by Meier et al. in view of Palekar et al., and further in view of Kalavade et al.

Paragraphs 18, 121, and 204 of Kalavade et al.

During the Examiner interview held between Examiner Chan and the undersigned on February 25, 2010, the Examiner requested paragraphs 18, 121, and 204 of Kalavade et al. be addressed regarding the patentability of Claim 1. The aforementioned paragraphs are repeated below for the Examiner's convenience.

> [0018] In accordance with one or more embodiments of the invention, a method is provided for allowing multiple wireless operators to provide integrated authentication and billing services for respective subscribers within one wireless LAN hotspot. The method includes: (a) modifying a hotspot authentication server to support multiple operators by assigning a separate network access identifier for each operator; (b) associating a gateway of each operator with each respective network access identifier; and (c) forwarding authentication requests received by the authentication server to appropriate gateways, depending on the operator selected by the user, each selected gateway providing authentication and billing for the selected user.[13]

> [0121] 3. The Access server at hotspot communicates with CBG server for authentication through RADIUS style protocol.[14]

> [0204] CBG interaction with other authentication systems at the hotspot location is now further described. The hotspot typically has its own authentication infrastructure in place. The CBG is designed to operate with this infrastructure. Most hotspots use a RADIUS server to provide authentication of its users. The RADIUS setup includes two main components: a network access server such as a router at a hotspot and a RADIUS server either at the hotspot or on the Internet. The network access server functions as a RADIUS client.[15]

Again, the above portions of Kalavade et al. speak generally about modifying a hotspot authentication server to support multiple operators by assigning a separate network access identifier for each operator, associating a gateway of each operator with each respective network access identifier, and forwarding authentication requests received by the authentication server to appropriate gateways, depending on the operator selected by the user, but nowhere do the cited portions of Kalavade et al. disclose or suggest determining, *by the network access device*, if the user device supports a user authentication protocol used by the host network as required by Claim 1. (emphasis added) The Applicant respectfully submits it is improper to equate modifying a hotspot authentication server to support multiple operators, with determining, by the network device, if the user device supports a user authentication protocol used by the host network as required by Claim 1.

[13] Kalavade et al. at ¶ 18.
[14] Kalavade et al. at ¶ 121.
[15] Kalavade et al. at ¶ 204.

Nor do the cited passages disclose or suggest placing, *by the network access device*, the port into a *semi-authorized access state* if it is determined that the user device does not support the user authentication protocol, the semi-authorized access state providing the user device with limited network access, as required by Claim 1. (emphasis added) The cited passages speak generally about authentication, but say nothing about a *semi*-authorized access state.

For at least the above reasons, the Applicant respectfully submits Claim 1 is allowable over the cited art of record. Withdrawal of the 35 U.S.C. § 103 rejection is respectfully requested.

Independent Claims 11, 20, 31

Claim 11 is a non-means-plus-function apparatus claim corresponding to method claim 1. Claim 20 is a non-means-plus-function system claim corresponding to method claim 1. Claim 31 is a means-plus-function apparatus claim corresponding to method claim 1. Claim 1 being allowable, Claims 11, 20, and 31 must also be allowable for at least the same reasons as for Claim 1.

Independent Claims 32, 36, and 41

Independent claim 32 is a method claim that includes limitations similar to independent method Claim 1. Specifically, Claim 32 as amended recites in part "*at the network access device*, allowing the user device limited access to a network via the network access device." (emphasis added) Accordingly, the arguments made above with respect to Claim 1 apply here as well.

Claim 36 is a non-means-plus-function apparatus claim corresponding to method claim 32. Claim 41 is a means-plus-function apparatus claim corresponding to method claim 32. Claim 32 being allowable, Claims 36 and 41 must also be allowable for at least the same reasons as for Claim 32.

Dependent Claims 2, 5-10, 12, 15-19, 21, 24-29, 33-35, and 37-39

Claims 2 and 5-10 depend from Claim 1. Claims 12 and 15-19 depend from Claim 11. Claims 21 and 24-29 depend from Claim 20. Claims 33-35 depend from Claim 32. Claims 37-39 depend from Claim 36. Claims 1, 11, 20, 32, and 36 being allowable, Claims 2, 5-10, 12, 15-19, 21, 24-29, 33-35, and 37-39 must also be allowable for at least the same reasons as for Claims 1, 11, 20, 32, and 36.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

The Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional required fee or credit any overpayment not otherwise paid or credited to our deposit account No. 50-3557.

Respectfully submitted,

NIXON PEABODY LLP

Dated: May 14, 2010

/John P. Schaub/
John P. Schaub
Reg. No. 42,125

NIXON PEABODY LLP
P.O. Box 60610
Palo Alto, CA 94306
Tel. (650) 320-7700
Fax. (650) 320-7701